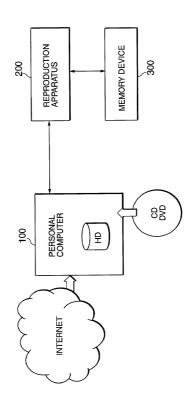
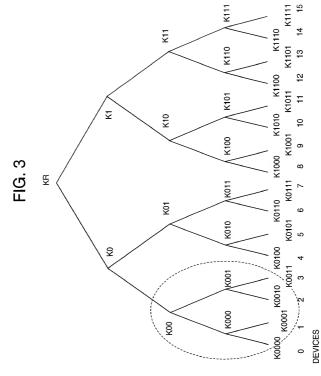


FIG. 2





EKB (ENABLING KEY BLOCK) EXAMPLE 1 DELIVERS NODE KEYS OF VERSION (t) TO DEVICES 0, 1,AND 2

VERSION: t	
INDEX	ENCIPHERING KEY
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

EKB (ENABLING KEY BLOCK) EXAMPLE 2 DELIVER NODE KEY OF VERSION (t) TO DEVICES 0, 1, AND 2

	VERSION: t	
	INDEX	ENCIPHERING KEY
(B)	000	Enc(K000, K(t)00)
(0)	001	Enc(K(t)001, K(t)00)
	0010	Enc(K0010, K(t)001)

(A)

FIG. 5

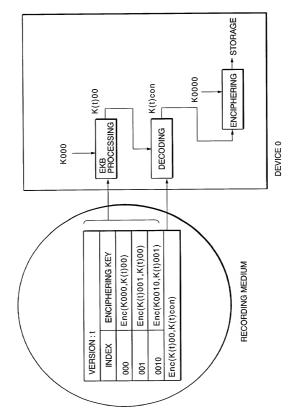
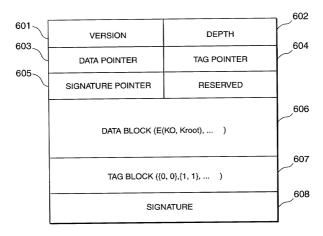
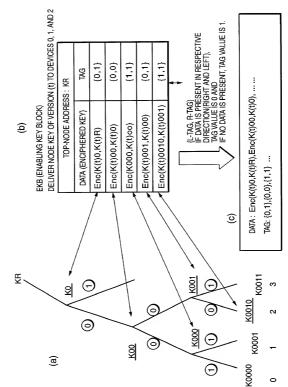
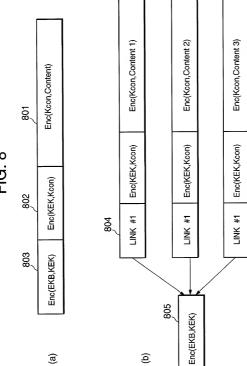


FIG. 6



F. '2





8/45

FIG. 8

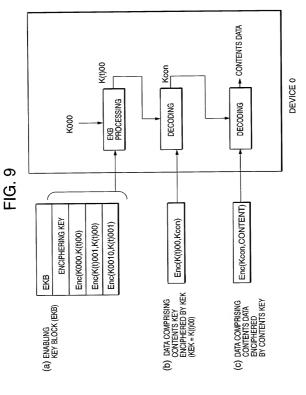
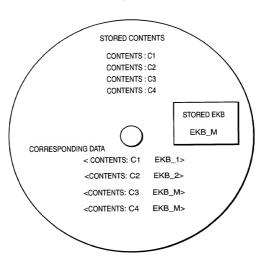


FIG. 10



RECORDING MEDIUM

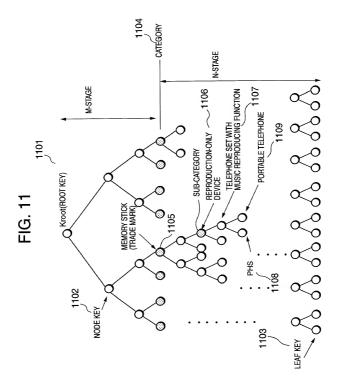


FIG. 12

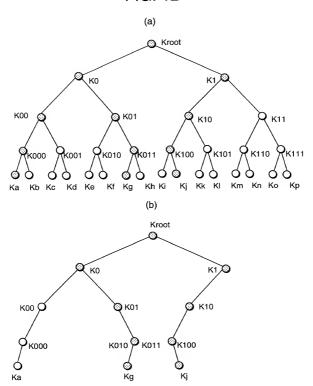
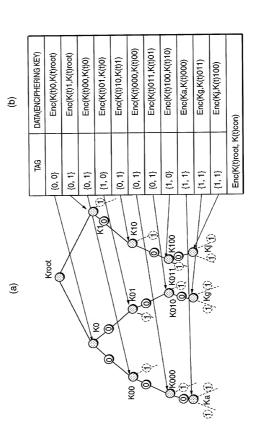
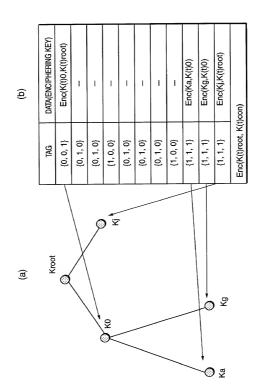


FIG. 13

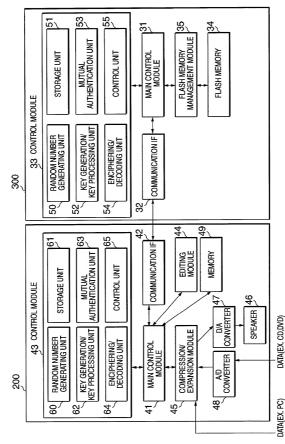


DOSTIONE DYNAMI

FIG. 14







DATA(EX. CD,DVD)

FIG. 16

DATA STORED IN A STORAGE UNIT OF A MEMORY DEVICE

	IK0
AUTHENTICATION KEY DATA	IK1
	IK2
	IK3
	:
	:
	IK30
	IK31
DEVICE IDENTIFICATION DATA	ID0
STORAGE KEY DATA	Kstm

FIG. 17

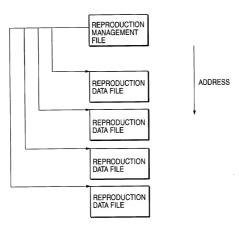
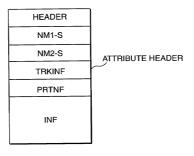


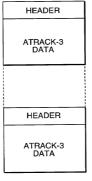
FIG. 18

REPRODUCTION MANAGEMENT FILE

HEADER
NM1-S
NM2-S
TRKTBL
INF-S

FIG. 19





REPRODUCTION MANAGEMENT FILE

A	A 0 .	1 2	3 4 5	6 7	8 9	АВ	СД	E F
0x0000 0x0010)-TLO		MCODE T-TRK	REVI VerNo.	SION	RESERVED	RVED
	3	SINZOTE	OIN OILL	11	70			
0x0020	NM1-S(25	56)						
0x0120	NM2-S(5	12)				-		
0x0310								
0x0320	RESER!			ERSION		E(Kstm		
0x0330		E(KEK				c_MA		
0x0340		RESE	RVED(8)			D(3) MGR		Dhms
0x0350	TRK-001	TRK-002	TRK-003	TRK-004	TRK-005	TRK-006	TRK-007	TRK-008
0x0360	TRK-009	TRK-010	TRK-011	TRK-012	TRK-013	TRK-014	TRK-015	TRK-016
0x0660	TRK-393	TRK-394	TRK-395	TRK-396	TRK-397	TRK-398	TRK-399	TRK-400
0x0670	INF-S(14	720)						
	,	•						
0x3FFF	BLKI	D-TLO	RESERVED	MCODE	REVI	SION	RES	ERVED

С	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F	
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	--

INF 0X00 ID 0X0	SIZE	MCODE	C+L	RESERVED	DATA VARIABLE LENGTH

ATRACK-3 DATA FILE

	0 1	2	3 4 5	5 6	7 8 9	9 A	вс	D E	F
0x0000	BLKID-H	IDO	RESERVED	MCODE	RES	ERVED	BLOC	K SERIA	
0x0010	N1C+L	N2C+L	INFSIZE	T-PRT	T-	SU	INX	XT	
0x0020	NM1-S(256	3)							
0x0120	NM2-S(512	2)							
									I
0x0310									
	RESERVED(ERSION			m, Kcon)		
0x0 3 30			n. Kcon)				/AC[n]		
0x0340			RVED(8)			_seq#	A LT		,
0x0350			AL-nnn(Upp			MG(D)SER			<u></u>
0x0360	CONN		YMDI	nms-S		nms-E	XCC CT		CN
0x0370	PRTS	SIZE			TKEY			ERVED(8)
0x0380			CONN			E(0x0388)		RTKEY	
0x0390	1117/2 2/2		l	RESE	RVED(8)		CO	OMUNN	
	INF(0x0400	J)							
0x3FFF	BLKID-	HDD	RESERVED	MCODE	RES	SERVED	BLO	CK SERIA	AL
0x4000	BLKID-	A3D	RESERVED	MCODE	CON	INUMO	BLO	K SERI	AL.
0x4010		BLOCK	SEED		IN.	NTIALIZAT	ION VECT	OR	
0x4020	SU-000(NE	3yte=384	Byte)						
0x41A0	SU-001(NE	Byte)							
0x4320	SU-002(NE	Byte)							
0x04A0	SU-041(NE	Byte)							
0x7DA0	RESERVE								
0x7F20		BL	SEED						
0x7FF0	BLKID-	A3D	RESERVED	MCODE	CON	NUMO	BLO	K SERIA	۱L

FIG 22

╙					
Ш	ERIAL	⇆			
۵	BLOCK SERIAL				
O	핆	×			ı
В		_			
٧	MED				
6	RESERVED	T-SU			
œ					
7					
0 1 2 3 4 5 6 7 8 9 A B C D E F	RESERVED MCODE	T-PRT			
5	Ω.				
4	ESERVE	INFSIZE T-PRT			
က	=	-			
Ø	8	N2C+L			
-	BLKID-HDO		<u>@</u>	(2)	-
0	BLK	N1C+L	NM1-S(256)	NM2-S(51	
	0000X0	0x0010	0x0020	0x0120 NM2-S(512)	0x0310

FIG. 23

		FNo		XCC CT CC CN
		ᆸ	WER)	CT
Kcon)	C[n]	٧	uuu(FO	XCC
E(Kstm, Kcon)	C_MAC[n]	INF_seq#	MG(D)SERIAL-nnn(LOWER)	YMDhms-E
EKB VERSION	E(KEKn, Kcon)	RESERVED(8)	MG(D)SERIAL-nnn(UPPER)	YMDhms-S
EK	E(KEK	RESE	ERIAL-n	
RESERVED(3) EKI			MG(D)S	MINNO
0x0320	0x0330	0x0340	0x0350	0×0360

Bit7: ATRAC3 Mode

0 : Dual 1 : Joint

Bits 6, 5, 4: N OF 3-Bit CORRESPONDS TO MODE VALUE

N	MODE	TIME	TRANSFER RATE	SU (SOUND UNIT)	Byte
7	HQ	47min	176kbps	31SU	512
6		58min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	MONO	181min	47kbps	119SU	136
0	MONO	258min	33kbps	169SU	96

Bit3: RESERVED

Bit2: DATA DISTINCTION 0: AUDIO

1: OTHERS

Bit0 : EMPHASIS

Bit1: REPRODUCED SKIP 0: NORMAL REPRODUCTION 1: SKIP 0: OFF

1 : ON(50/15 μ SECCOND)

Bit7: COPY APPROVAL 0: COPY INHIBITED 1: COPY APPROVED

1: BEYOND THE FIRST GENERATION Bit6: GENERATION (VERSION) 0: ORIGINAL

Bits-4: CONTROL IN RELATION TO HIGH-SPEED DIGITAL COPYING OPERATION HCMS CHILD WHO IMPLEMENTED COPYING OF THE FIRST GENERATION IS INHIBITED FROM EXECUTING FURTHER COPYING OPERASTION

Bit3-2: MAGIC GATE AUTHENTICATION LEVEL

00: LEVEL10(Non-MG) 01: LEVEL1 02: LEVEL12 11: RESERVED

02: LEVEL12 11 : RESERVED 02: LEVEL10 11 : DESERVED 12: LEVEL10 11 : DESERVED NOT BE DIVIDED NOR COMBINED 14: DESERVED NOR COMBINED 14: DESERVED NOR COMBINED 15: DESERVED NOR COMBINED NOR

Bit1, 0: RESERVED

DOGITORS STREET

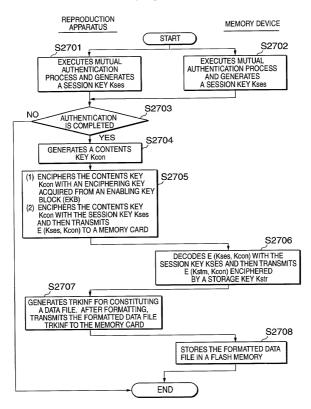
FIG. 26

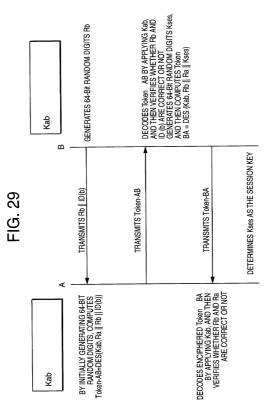
0x0370	PRTSIZE	PRT	PRTKEY	RESERVED (8)
0×0380		CONNUMO	PRTSIZE(0x0388)	PRTKEY
0×0390		RESE	RESERVED (8)	CONNUMO

FIG. 27

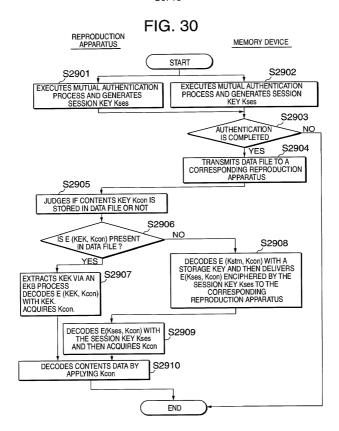
0×4000	BLKID-A3D	RESERVED MCODE	MCODE	CONNUMO	BLOCK SERIAL
0x4010	BLOCK	BLOCKSEED		INTIALIZATI	INTIALIZATION VECTOR
4020	0x4020 SU-000(NByte=384Byte)	yte)			

27/45





MUTUAL AUTHENTICATION FORMAT AND KEY.COMMUNIZING FORMAT VIA UTILIZATION OF THE ISO/IEC9798-2 STANDARD SYMMETRICAL KEY ENCIPHERING ART



TOOTIONS TOOTS

EIG.

⊥																		
ш	ĮN N																	
C D E	LINK COUNT																	
ပ	=	VED(8		(NOIS														
В	ŔΕ	RESERVED(8)	KEK1	E(VERSION)	¥.	÷												
∢	(S)	В		E	IN PA													
6	RESERVED(3) LKF				JF SIG	: : ⊢												
8	RESE				SIZE OF SIGN PART	, (X,1,	KEY PART	SIGNATURE										
7	_	\vdash				0,0} LIG	EY P	IGNA										
9	MCODE		RESERVED		SIZE OF KEY PART	TAG PART ((X,O,O), {X,1,1}) FILL TO 64Bit ALIGNMENT		S										
2			EA KEK2		F KE	F KE	F KE	F KE	F KE	유	F KE	Ä	G PA					
4	RESERVED	(8) ED(8)		TA TA	≱∄													
8 4	뿐	RESERVED(8)										Æ	A	EK2	H			
Ø	<u>в</u>											~	PART					
0 1 2	BLKID-EKB		VERSION		- TAG													
0	岩		>		SIZE OF TAG PART													
	L	. 0	٩	<u></u>	<u> </u>													
	0000x0	0x0010	0x0020	0x0030	0x0040	0x0050												

FIG. 32

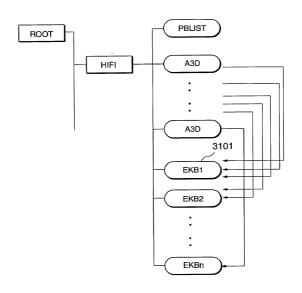
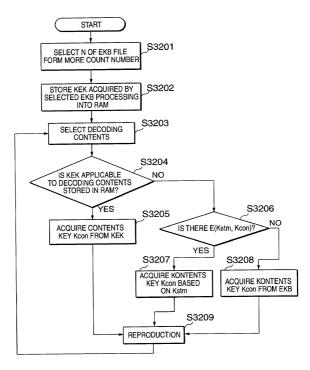


FIG. 33





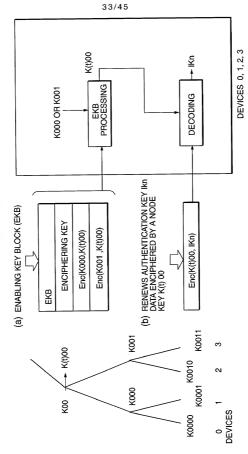


FIG. 35

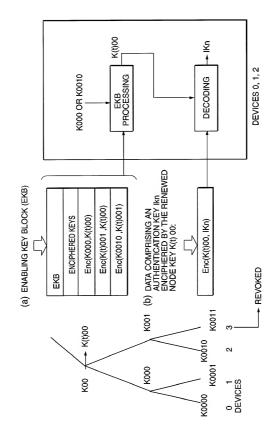


FIG. 36

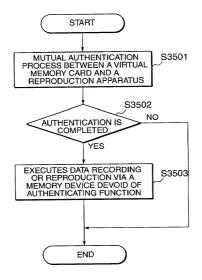
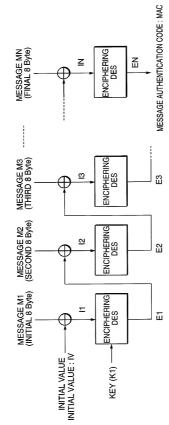
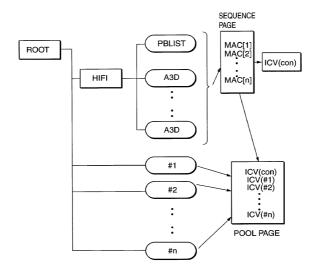


FIG. 37



EXCLUSIVE OR PROCESS (8 Bytes UNIT)

FIG. 38



DWGIIONE DZEEGI

	<u>ш</u> [_	\neg	_	
	Ш					REVISION
	CD		IO(LOWER)			REVI
				Ξ	[3]	
	В			C_MAC[1]	C_MAC[3]	
	A	ш	2	O	٥	Œ
RMAT	6					RESERVED
용	œ					-
SE PA	7					 -
SEQUENCE PAGE FORMAT	9				C_MAC[2]	
	2					
	4			C_MAC[0] (PUBLIST)		_
	က	(con)	ID(Upper)			Cinnr
	8	E(Kstr, Kcon)	[Ğ [Ğ	AC[0]	S S	C MACInnni
		Ш		O		
	0					
	0					
		L	L	_	<u> </u>	L
		0000x0	0x0010	0x0020	0x0030	0x0FE0

38/45

FIG 40

	1	_					
	۲						
	ш						
						(
	<u>۵</u>	Kicv)		Kicv)		, Kic	ا. ـ
	В	#0_E(KEK, Kicv)	ICV0	#1_E(KEK, Kicv)	ICV1	#15_E(KEK, Kicv)	ICV15
	٧	#0_E(_	#1_E	Γ	#15_E	
-	6	,-					
RMA							
出	8						
POOL PAGE FORMAT	7	NO		S		S	
8	9	#0_EKB VERSION		#1_EKB VERSION		ERSI	
	2	EKB V		Ϋ́Β V		KB V	
	4	#0_E	Šić.	#	(icv)	#15_EKB VERSION	,Kicv
	က		Ê,		KEK.	-	Α Ā
	7	NO	#0_E(KEK, Kicv)	S N	#1_E (KEK, Kicv)	#15_REVISION	#15_E (KEK, Kicv)
	0 1 2	#0_REVISION	#	#1_REVISION	#	REVIE	#
	_	#0_R		# #		#15	
	J						
		_ 8	9	50	90	 	6
		0000x0	0x0010	0x0020	0x0030	0x01E0	OXOTEO

FIG. 41

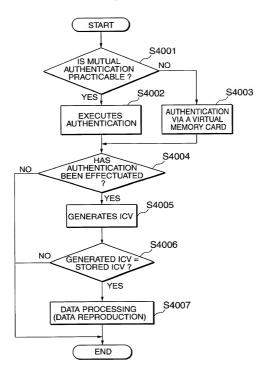


FIG. 42

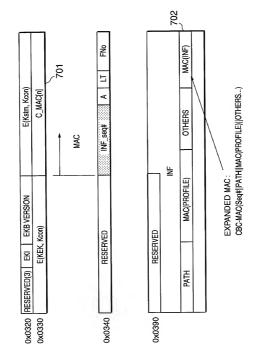


FIG. 43

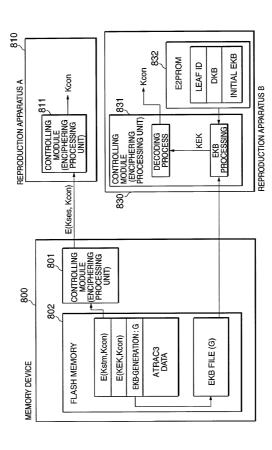
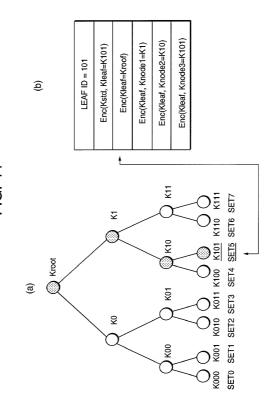


FIG 44



43/45

@

LEAF ID = 101

Enc(Kleaf, Kn47)

Enc(Kleaf, Kn46)

:
:
:
:
:
Enc(Kleaf, Kn8)

